

Nyáry Gábor

Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái

Bevezetés

2020 májusában, amikor az új koronavírus-világjárvány első hulláma kicsit engedett szorításából, szükséztű hírt jelent meg.¹ A korábbi hónapok drámai bejelentéseihez képest ártatlannak tűnő szövegre azonban okkal figyeltek fel a szakemberek. Az amerikai Szövetségi Nyomozó Iroda, az FBI és a Kiberbiztonsági és Infrastruktúra Védelmi Hatóság a Kínai Népköztársasághoz köthető kibernemzetek fokozott aktivitására figyelmeztettek. Az állami és a magánszférába tartozó „érdeklődők” a Covid-19-járványhoz kapcsolódó kutatási adatokat és szellemi tulajdont igyekeztek illegálisan megszerezni. Amerikai egészségügyi intézmények, gyógyszergyárak, kutatólaboratóriumok hálózatait támadva azonosították, gyűjtötték a koronavírus-vakcinákkal, -gyógyszerekkel kapcsolatos létfontosságú információkat.² Más szóval nemzetbiztonsági adatokat. Ám ezek az adatok, joggal mondhatjuk, ugyanakkor roppant üzleti értéket képviselő, gazdasági információk is. A 21. századi kibervalóság fontos mozzanata éppen ez: a kibertér egyszerre országok közötti politikum és nemzeteken átívelő gazdasági terep. Amikor „kiberbiztonságról” beszélünk, szinte mindig gazdasági vetületeket is érintünk alatta. És viszont: az egyre inkább digitalizálódó, globális „kiber-gazdaság” mindig egyfajta biztonsági téma is. Biztonság és gazdaság – a kibertér két oldala. A kibertér mint gazdasági mező, üzleti érdekek és ambíciók egyszerre virtuális és nagyon is valóságos térsége ma még kialakulóban van:

¹ FBI–CSISA PSA PRC Targeting of COVID-19 Research Organisations. 2020.

² A kiberdiplomácia elismert kutatóbázisa, a genfi DiploFoundation havi jelentése egyenesen úgy fogalmazott: „A világban a kiberbűnözés is visszatért a szokványos kerékvágásba.” A kutatócsoport is egyértelműen jelezte: a kibertérben megszaporodott támadások többsége kórházak, kutatóintézetek ellen irányul, alapvetően a gazdasági kibertérhírszerzés és kibertolvajlás eseteit szaporítva. A primer „nemzetbiztonsági” vagy politikai jellegű kiberakciók mintha háttérbe szorultak volna, noha az akciókban részt vevők között szép számmal akadnak állami aktorok is. *Digital Watch Newsletter*. 2020.

evolúcióját, fejlődési irányait, szabályozási kereteit ma még kérdések, élénk nemzetközi viták kísérik. Minden jel arra mutat: a kibertér mint gazdasági szféra dilemmái a kiberdiplomácia napirendjének fő tételei maradnak még egy időre.

Digitális geoökonómia

Kötetünk bevezető tanulmányában a kibertér geopolitikai értelmű koncepcióját igyekeztünk bemutatni. Elsőnek említettük, hogy úgy tekinthetünk a kibertérre, mint az internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mindinkább hálózatokba szerveződő alkalmazók összességére. Ehhez hozzátettük a korszak (ismét divatba jövő) hatalmi-politikai koncepcióját, a geopolitika fogalmát, amely lényegét tekintve azt hangsúlyozza: a nemzetek egymás közötti viszonyát, érdekérvényesítési mozgásait nagymértékben befolyásolják bizonyos hosszú távon állandó struktúrák. Elsősorban persze maga a környezet, a fizikai tér: az ország elhelyezkedése, domborzati viszonyai, vízrajza, népesedésföldrajza.³ Most, a kibertér gazdasági aspektusait szemügyre véve, elérkezettnek látjuk az időt arra, hogy ezzel az újabb vetülettel bővítsük koncepciónkat. Azzal a területtel, amelyet talán a digitális geoökonómia fogalma írhat le a legjobban.⁴

Keretek és fogalmak

Ha korábban (e kötet bevezető fejezetében) siettünk hangsúlyozni, hogy a „geopolitika” kifejezés távolról sem rendelkezik valamilyen egységes, mindenki által elfogadott jelentéstartalommal vagy akár használattal, akkor még erőteljesebben érdemes most figyelmeztetni rá: az általunk bevezetett újabb szóösszetétel, a „geoökonómia” sincsen jobb helyzetben. Sőt! Sokan, sokféle jelentésárnyalattal

³ Nyáry Gábor: Kiber geopolitika. Mesterséges intelligencia alkalmazások az államigazgatás külpolitikai alrendszerében. *Új Magyar Közgazdaság*, 13. (2020), 1. 32–39.

⁴ A koncepciónak nincs túlságosan kiterjedt szakirodalma (összevetve legalábbis a geopolitika fogalomkörével). A probléma egyik legkitűnőbb exponálására vállalkozik Sami Moisoio: Re-Thinking Geoeconomics: Towards a Political Geography of Economic Geographies. *Geography Compass*, 13. (2019), 10. 1–13. Ugyanakkor magyar nyelven ad kiváló betekintést és általános háttérter Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

alkalmazzák: vannak, akik létjogosultságát is vitatják, de az mindenesetre jól látható, hogy még a szakmai közbeszédben sem tudott annyira gyökeret verni, mint rokona, a „geopolitika”.⁵ Pedig a „geoökonómia” – noha a szóösszetétel valóban kicsit félrevezető lehet – rendkívül pontos és fontos meglátást takar. Érdemes ehhez felidézni azt a szerzőt, aki a világpolitika tektonikus átalakulásának időszakában, az 1990-es évek legelején (ismét) divatba hozta az elképzelést. Edward Luttwak, a stratégiaelmélet és stratégiatörténet egyik sokat kritizált, de kétséget kizáróan legeredetibb gondolkodója nyers őszinteséggel fogalmazta meg a kor egyre szembeötlőbb jelenségét: a gazdaság, és különösen a nemzetközi gazdaság – valójában harc, háború. Ennek a háborús jellegnek az érzékeltetésére vezette be a geoökonómia fogalmát.⁶ Ugyanakkor ez az időszak volt az a történelmi pillanat, a hidegháború vége, amikor sokan gondolták úgy, hogy az államok közötti konfliktusok katonai megoldása örökre a múlté lett.⁷ Luttwak geoökonómia-kifejezése azt hangsúlyozza: immár a katonai erő helyett a gazdaság, a nemzetközi kereskedelem eszköztárával vívják majd küzdelmeiket a rivális világhatalmak. Akár úgy is fogalmazhatunk: a geoökonómia szűkebb jelentéstartalmú, mint a fegyveres erőszakot is magába foglaló geopolitika, ám a pusztán külgazdasági kapcsolatrendszerénél szélesebb.⁸ Az elképzelés jogosságát, használhatóságát és időtálló jellegét jól bizonyítja a világ globális nagyhatalma, az USA 2017-es Nemzetbiztonsági stratégiája, amely precíz erővel mondja ki: a gazdaság biztonsága – nemzetbiztonsági kérdés.⁹ Ha most egy pillanatra felidézzük a jelen fejezet bevezető gondolatai között említett mostani példát, ahol állami szereplők igyekeznek nemzetbiztonsági horderejű üzleti titkokat megszerezni és eltulajdonítani a kibertérben, akkor kezdjük látni, hogyan kapcsolódnak egymásba ezek a körök.

⁵ Mihael Wigell et al. (szerk.): *Geo-economics and Power Politics in the 21st Century* (London, Routledge, 2019) a terminológiai kérdések áttekintése mellett a koncepció jól alkalmazható leírását adja.

⁶ Edward Luttwak (From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest*, [1990], 20. 17–23.) későbbi követői tovább is léptek a történelmi parafrázisgyártás terepén, és egyenesen a 19. századi nagy porosz katonai gondolkodó, Clausewitz híres mondatát fogalmazták át így: „A gazdaság a háború folytatása más eszközökkel.”

⁷ Nem véletlenül éppen ez az a pillanat, amikor például megszületik – az amerikai politikatudós Joseph Nye tollából – a nemzetközi kapcsolatok elméletének egyik leghíresebb koncepciója, az államok békés érdekérvényesítését hangsúlyozó *soft power* fogalma.

⁸ Franz-Stefan Gady: *Interview: Robert Ward and Yuka Koshino on Geo-Economics in East Asia*. 2020.

⁹ Gady (2020): i. m.

A kibervilág mint a politikum színtere – ezt a felfogást igyekszik megragadni a „kibergeopolitika” koncepciója (erről szoltunk részletesen e könyv bevezető fejezetében). Létezik azonban egy másik dimenzió, ahol a kibertér mint gazdasági-üzleti folyamatok színtere jelenik meg. Ez a „kiber-geoökonómia” (vagy digitális geoökonómia) területe. Alapvetően ez határozza meg a digitális gazdaság jellegét, működési módjait, folyamatait.

Digitális gazdaság

Digitális gazdaságot mondtunk, és okkal: ma már a szakmai nyelv bevett kifejezésévé vált ez a szókapcsolat. A 2000-es évek elejétől ugyanis érezhetően gyorsuló tempójú jelenség formálja a világ szinte valamennyi társadalmát: a digitalizáció. Sommás megfogalmazással úgy jellemezhető ez a folyamat, mint amelyben az adatok és a hálózatok körbefonják, átítatják a termelési folyamatokat, a kormányzati és személyes fogyasztást, a határokon átvélő kereskedelmi forgalmat és természetesen a gazdaságot mozgató pénzügyeket is.¹⁰ Nemi óvatosság azonban nem árt! A „digitális gazdaság” kifejezés, nyilvánvaló jelentéstartalma ellenére, tudományos értelemben nem egységes koncepció, nem elfogadott definíció. A globális gazdaságstatisztikákban megkerülhetetlen Nemzetközi Valutaalap a digitális gazdaság teljesítményéről szólva leszögezi: még abban sincs teljes egyetértés, hogy mit értsünk a gazdaság „digitális szektorán”, vagy miket soroljunk a „digitális termékek” körébe. Noha a szakmai beszédben mára teljességgel polgárjogot nyert, és így mi is használjuk a „digitális gazdaság” fogalmát, ne vesszünk szem elől, hogy ez még egy alakuló, formálódó koncepció, folyamatosan bővülő jelentéstartalmakkal.¹¹

¹⁰ *Measuring the Digital Economy*. 2018. 6. A téma friss áttekintését adja Vladimir M. Filippov et al. (*The Cyber Economy. Opportunities and Challenges for Artificial Intelligence in the Digital Workplace*. Cham, Springer Nature, 2019), aki rávilágít arra, hogy a meglehetősen következetlen fogalomhasználat csak tovább bővül azzal, hogy a korábbi „internetgazdaság” kifejezés helyébe mind gyakrabban lép az „ipar 4.0” fogalom is, tehát a dolgok internete (Internet of Things – IoT) által forradalmasított és átalakított gazdaság.

¹¹ *Measuring the Digital Economy*. 2018. A pontosság kedvéért érdemes megjegyezni, hogy a nemzetközi statisztikák, egyebek mellett az ENSZ gazdaságstatisztikai rendszere, „információs és kommunikáció technológiai (IKT-) szektorról” beszél, valamint egy „tartalom- és médiaipari szektorról”. A kicsit szabadabban vett szakmai közbeszéd nagyjából e két kategóriához sorolható fogalomkészleteket érti a „digitális gazdaság” alatt.

A definíció feljebb ismertetett nehézsége miatt a számadatokkal is óvatosan érdemes ugyan bánni, de a digitális gazdaság teljesítménye, fejlődési üteme így is figyelemre méltó. Mértékadó számítások szerint a digitális gazdaság aránya a világ gazdaság összteljesítményén belül eléri a 22,5%-ot.¹² A digitalizáció terén hagyományosan az élen szereplő Egyesült Államok 5,9 billió dolláros digitális gazdasága az ország GDP-jének mintegy 33%-ára rúg. A szakemberek különösen fontos szerepet, gazdaságnövekedési motort látnak a digitális befektetésekben: ez az USA-ban, 2020-ra számítva, további 2,2%-os GDP-növekedést eredményez.¹³ A digitalizáció terjedésének, a digitális gazdaság növekvő potenciáljának kihasználásához elengedhetetlen az IKT-technológiák széles körű társadalmi befogadása és abszorpciója is. A digitális gazdaságban rejlő lehetőségek kiaknázására való képességet mutatja a Világ gazdasági Fórum Hálózatos Készenléti Indexe (NRI), ahol az Egyesült Államok már csak az 5. helyen áll, előtte Szingapúrral, Finnországgal, Norvégiával és Svédországgal.¹⁴

Kiberbiztonság és nemzetközi kereskedelem

Az üzlet, a gazdaság ma már ezer szálon kapcsolódik az internethez, az IKT-technológiákhoz. Az országhatárokon átnyúló, nemzeteket összekötő külkereskedelem esetében pedig ma már nem mozdulhat áru vagy szolgáltatás a kibertér (valamilyen formában történő) érintése nélkül. A kibertér szabályozási, kormányzási-igazgatási kérdéseivel foglalkozó kiberdiplomácia fókuszában éppen ezért egyre előkelőbb helyre kerülnek a kereskedelem, sőt általában véve a digitális

¹² Chooi Shi Teoh – Ahmad Kamil Mahmood: National Cyber Security Strategies for Digital Economy. *Journal of Theoretical and Applied Information Technology*, 95. (2017), 23. 6510–6522. 6511. A számítások természetesen eltérő eredményeket hoznak. A Foreign Policy folyóirat adatkormányzásról, nemzetközi kiberdiplomáciai és szabályozási törekvésekről szóló friss összefoglalója például a globálisan előállított GDP 15,5%-ára teszi a digitális gazdaság teljesítményét. Jellemző adat azonban ezen belül is: a nagy internetes platformok (mint a Google, Facebook, WeChat stb.) együttes értéke teszi ki a világ GDP-jének csaknem 10%-át. *Data Governance. Part I. Emerging Data Governance Practices*. 2020.

¹³ Teoh–Mahmood (2017): i. m. 6511.

¹⁴ Teoh–Mahmood (2017): i. m. 6511.

gazdaság és a kibertér kapcsolódási területein felbukkanó kockázatok, problémák.¹⁵

Közhely már lassan, de érdemes sokadszorra is hangsúlyozni: a modern gazdaságokban egyre nagyobb szerepet kap az adat; sőt hovatovább meghatározóvá válik a szerepe. Nem véletlenül élnek gyakorta az új fordulattal: az adat a 21. századi gazdaságok „olaja”. Az adat pedig, nem mondunk ezzel meglepőt, a kibertérben él, ott sokasodik, ott mozog. Ahogy bővül (még hozzá exponenciális sebességgel) a világban felhalmozódó adattömeg, ahogy terjeszkedik, bővül a digitális gazdaság – egyre növekszik a kiberbiztonsági kockázatok abszolút és relatív mértéke.¹⁶ A digitális gazdaság, és különösen az élenjáró technológiák, az adatok tömegének határokra átnyúló globális áramlásától függenek ma már: az adat élteti az innovációt, adatokon alapul a termelőeszközök beszerzése, és adatok teszik lehetővé a késztermékek és szolgáltatások kiszállítását is. A mesterséges intelligencia (a továbbiakban: MI), az elkövetkező évtizedek nagy ígérete adatok, még hozzá hatalmas adattömegek nélkül semmire sem menne. Az MI-technológiák egyik legfontosabb területét jelentő gépi tanuló rendszerek például hatalmas adattömegeken „treníroznak”. Ezeknek az adatoknak egy része ma már a globális digitális hálózatokon át jut felhasználási helyére.

De ott van az e-kereskedelem, amelynek révén nem csupán a gazdasági élet mamutjai, de kis- vagy akár mikrovállalkozások is szerves kapcsolatba léphetnek a kibertérrel. Az elektronikus kereskedelemben is az adat az éltető elem, és ez az esetek jó részében itt is globális forgalmat jelent. Az Egyesült Államokban például a közismert eBayre felcsatlakozott kisvállalatok 97%-a exportál is, azaz aktívan kapcsolódik be a nemzetközi kereskedelmi forgalomba.¹⁷ De ma már az internetes hozzáférés és a határokon átívelő adatáramlás jellemzi a szolgáltató szektor jelentős szeletét is. A szolgáltatások egyre nagyobb hányadát adják és veszik online hálózatokon át.

¹⁵ Pascal Brangetto et al. (*Economic Aspects of National Cyber Security Strategies. Project Report*. Tallin, CCDCOE, 2015) egyik fő erőssége, hogy az egyes nemzeti kiberbiztonsági stratégiák explicit gazdasági vetületeit veszi számba, amire viszonylag kevés példa akad a szakirodalomban.

¹⁶ Joshua Meltzer: *Cybersecurity, Digital Trade, and Data Flows. Re-Thinking a Role for International Trade Rules*. 2019. 7. Ugyanakkor a téma átfogó áttekintéséhez, az elsődlegesen biztonsági fókuszú kiberbiztonsági koncepciók egyre erőteljesebben jelentkező gazdasági összefüggéseikhez itt találunk rendkívül hasznos adalékokat: Brangetto (2015): i. m.

¹⁷ Meltzer (2019): i. m. 5.

A digitális gazdaságot és a globális adatáramlást fenyegető kiberfenyegetések öt nagyobb területet ölelnek fel.¹⁸ Az első terület maga a nemzetbiztonság térrendszere: a fegyveres erők, a nemzetbiztonsági szervezetek. A második nagyobb terület, ahol a kibertér fenyegetései ma már több mint kézzelfoghatóak egyes esetekben, a kritikus infrastruktúra területe. A harmadik nagyobb fenyegetési terület az üzleti-kereskedelmi titkok területe. A negyedik olyan terület, ahol a kiberválóság fenyegető árnya tornyosul, az egyéb online információk hatalmas gyűjtőterülete. És van még egy ötödik tér, ahol a kiberfenyegetésekkel szembeni sérülékenység gyors tempóval növekszik: a nemzetközi befektetésekre vonatkozó (kulcsfontosságú) információk szintén hatalmas tere. Ebben az összefüggésben érthető, hogy az államokra egyre nagyobb mértékben nehezedik a magángazdaságba tartozó szereplők kiberbiztonságának védelme, garantálása, amiből a kiberdiplomácia struktúrái is kiveszik a részüket.

Érdemes egy pillanatra kitekinteni: a kiberincidensekkel, kibervédelemmel kapcsolatos híradásokban – érthető módon – a nemzetbiztonsági, politikai jellegű akciók és események kapnak különös hangsúlyt.¹⁹ Ugyanakkor, ha a bevezetőben említett, gyógyszeripari információszerző kiberakciókon elgondolkodunk, és szemügyre vesszük az (ismertté vált) ilyen incidensek folyamatosan bővülő listáját, akkor jól látható tendencia bontakozik ki a szemünk előtt.²⁰ Érzékelhetően növekszik a gazdasági jellegű kiberakciók mennyisége és az ilyen támadások intenzitása. A jelenség nagyobb időtávban szemlélve is ehhez hasonló képet mutat: gyors pillantást vetve például a CSIS vezető agytröszt fontosabb kiberakciókat rögzítő listájára, viszonylag nagy számban sorjáznak rajta a gazdasági jellegű beavatkozások.²¹ A témával kapcsolatban van olyan kutató, aki egyenesen a gazdasági kiberkémkedés aranykorát jósolja, illetve egyfajta aranylázhoz hasonlítja a virtuális terekben felerősödő, ipari-, pénzügyi-, gazdasági-, technológiaiinformáció-szerző aktivitást.²² A kiberkémkedéssel foglalkozó szakirodalom ezt a felfelé ívelő trendet egészen a hidegháború végéig vezeti vissza. Többről van szó véletlen egybeesésnél, hogy a geoökonómia, tehát a nemzetközi gazdasági kapcsolatok fegyverként való használatának koncepciója éppen akkor

¹⁸ Meltzer (2019): i. m. 8.

¹⁹ Joyce Hakmeh: *Cybercrime and the Digital Economy in the GCC Countries*. London, Chatham House, 2017.

²⁰ *Covid-19 Cybercrime Weekly Update*. 2020.

²¹ *Significant Cyber Incidents*. 2020.

²² Danilo D' Elia: La Guerre économique à l'Ère du Cyberspace. *Hérodote*, 152–153. (2014), 1–2. 240–260. 243.

vert gyökeret, amikor a gazdasági előnyöket szem előtt tartó kibertevékenységek is sokasodni kezdtek.²³ Figyelemre méltó jelenség továbbá az is, hogy amíg korábban döntően állami szereplőkhöz kapcsolták a gazdasági jellegű kiber(kémkedési) akciók többségét,²⁴ addig az utóbbi évtizedekben stabilan erősödik a nem állami szereplőkhöz kapcsolható, gazdasági előnyszerzésért indított kiberhadműveletek aránya.

A fentiek fényében nem meglepő, hogy a kibertér vonatkozásában a „biztonság” és a „gazdaság” szféráinak egyre jobban kitapintható átlapolódásáról, összeolvadásáról beszélnek.²⁵ Összességében kijelenthető, hogy a kibertér egyre meghatározóbb szerepet játszik a nemzetközi kereskedelemben.²⁶ A kiberbiztonsággal kapcsolatos aggodalmak, beleértve a nemzeti és nemzetközi ellátási láncok épségével kapcsolatos kiberbiztonsági félelmeket is, arra sarkallják az államokat és a magánszféra szereplőit egyaránt, hogy hatékony lépéseket tegyenek a kibertér biztonságának megóvásáért. Egymást követően jelennek meg az újabb irányelvek és szabályozási keretrendszerek, amelyek gyors tempóban alakítják át a nemzetközi kereskedelmet. Újabb mechanizmusok és megállapodások formálódnak, amelyek a kibertér konfliktushelyzeteinek a feloldását célozzák, és hozzájárulnak a potenciális kiberbiztonsági fenyegetések csökkentéséhez. Érdemes itt kiemelni egy sajátos szegmenst, már csak azért is, mert a 2020-as év elejének globális egészségügyi krízise különösen ráirányította a témára a világközvélemény figyelmét. A globális pandémia, a koronavírus-járvány különös élességgel mutatta meg a globalizálódott gazdaság egyik legfontosabb tényezője, a globális ellátási láncolatok nagyfokú sérülékenységét. A kiberbiztonság és a kereskedelem összefüggéseit kutató szakemberek most különösen határozottan mutatnak rá a globális (és nemzeti) ellátási láncolatok kiberbiztonsági kérdéseinek fontosságára. Egyértelműnek látszik a konszenzus abban, hogy – ha az elkövetkező időszakban nem történik számottevő elmozdulás a kibertérben

²³ Russell Buchan: *Cyber Espionage and International Law*. Oxford, Hart, 2019. 23.

²⁴ A teljességhez hozzátartozik az is: az 1990-es évektől felerősödő, állami szereplők által folytatott gazdasági célú kiberakciók egy jelentős részében is a magánszektor gazdasági szereplői lettek a megszerzett információk „kedvezményezettjei”.

²⁵ A nemzetközi kereskedelem erőteljes „felköltözése” a kibertérbe a korszak egyik igazán jellemző vonásaként értékelhető. Nem véletlen, hogy az államok közötti kiberkonfliktusok egy nem jelentéktelen része már most is a globális kereskedelmi ügyletekhez és csatornákhöz kapcsolódik. *International Trade Regulation and Cybersecurity* (é. n.).

²⁶ Keman Huang et al.: *Interactions between Cybersecurity and International Trade: A Systematic Framework*. Cambridge, MIT Sloan, 2018. 45.

való viselkedés normarendszereinek kialakításában – az ennek nyomán sokasodó kiberkonfliktusok és kiberincidensek rendkívül károsan érintik majd a nemzetközi kereskedelem egészét.²⁷ A kiberdiplomatakon tehát ezen a rendkívüli fontosságú gazdasági területen is nagyon sok múlik majd.

A digitális gazdaság dilemmái

A kibervilág, különösen annak gazdasági dimenziója, ma még képlékeny és formálódó terület. Olyan térsége a nemzetközi kapcsolatoknak, ahol több fontos kérdésben ellentétes felfogások és érdekek feszülnek egymásnak. És a tét óriási. Sokszor ezek a viták elvi jelentőségűnek tűnnek, pedig a valóságban jól tapinthatóan ott húzódnak a póre gazdasági célok és érdekek. Ezért is gondoljuk azt, hogy ezeket a témákat itt, a kibertér gazdasági viszonyainak ismertetésekor indokolt körbejárni. Két különböző probléma, két egymással ellentétes attitűd, magatartás, szabályozási törekvés érdemel ebben az összefüggésben említést, de közös bennük: a digitális gazdaság mindkét nagy kérdéssoportja valójában az „adat” körül forog, az adatról szól.²⁸ Az ok végül is könnyen érthető: ebben a modern gazdaságban már nem a fizikailag létező javak, termékek előállítása, forgalmazása, szállítása, vásárlása és fogyasztása a meghatározó. A számítástechnikai rendszerek terjedésével óriási tömegű információ generálása, feldolgozása, tárolása, változatos célú továbbhasznosítása, a hálózatokon (elsősorban az interneten) keresztüli továbbítása az, ami a gazdasági értékteremtő folyamatok központi mozzanatává válik. Az adat tehát az új erőforrás, ténylegesen egyfajta nyersanyag, ezért megszerzése, birtoklása, használata, feldolgozása hasonló kérdéseket vet fel, mint az ipari gazdaságok „hagyományos” nyersanyagainak esete. Az „adat” fogalmán itt általában különlegesen nagy adattömegeket értünk, ezek megjelölésére szolgál az úgynevezett *big data* fogalom.²⁹ Az adat különleges tulajdonságát, megváltozott gazdasági szerepét mutatja az is, hogy az illetéktelen

²⁷ Huang (2018): i. m. Az MI-technológiák alapvetően stratégiai jellegű orosz megítélésére és jelentőségére lásd még David Meyer: *Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World*. *Fortune*, 2017. szeptember 4.

²⁸ Barbara Roseb Jacobson – Katharina E. Höhne – Jovan Kurbalija: *Data Diplomacy*. Genf, DiploFoundation, 2018 kiváló, tömör áttekintését adja az adatok digitális gazdaságon belüli szerepének és a felmerülő szabályozási kérdéseknek.

²⁹ Az IBM informatikai óriáscég becslése szerint világunkban naponta mintegy 2,5 exabit adat keletkezik, amit egy szám után álló 18 nullával lehet kifejezni. Ennek az óriási mennyiségű adatnak

eltulajdonítás (magyarul adatlopás) a kiberbűncselekmények egyik jellemző válfajává kezd válni.³⁰ Az adat tehát érték, és a roppant sok adat roppant nagy gazdasági értéket képvisel.

Az internet szabadsága és a kiberzsuverenitás mint gazdasági szempont³¹

Az egyik legjobban exponált (és kétségtelenül a legnagyobb horderejű) dilemma így hangzik: „az internet szabadsága” vagy a „kibertér szuverenitása”? Melyik volna a kívánatosabb?³² A probléma gyökere tulajdonképpen a kibertérnek, ennek a furcsa technológiai-társadalmi-politikai struktúrájának a különlegességében gyökerezik. A fogalomhoz ugyanis szinte születésétől fogva erősen kötődik annak „közlegelő” felfogása. Nagyon erős a vélekedés, hogy a kibervalóság egyfajta „digitális köztulajdon”: olyan, mint az iparosodás előtti idők falusi társadalmainak közösen használt javai, az erdők, a halászó vizek, a legelők. Geopolitikai értelemben szemlélve olyasmí, mint a nyílt óceán vagy a világűr. Az internet szabadsága, vagy más megfogalmazással a netsemlegesség mellett lándzsát török ezt a felfogást képviselik, és a kibertér nemzetközi szabályozását, szabályozottságát (tehát korlátait) igyekeznek a lehető legcsekélyebb mértékűre szorítani.³³ Ezzel ellentétben azonban létezik egy másik felfogás, egy másik vízió arról, hogyan kellene kinéznie és működnie ennek az egyszerre virtuális és nagyon is kézzelfogható világnak. A „kibertér szuverenitása” mellé állók azt az elvet tartják követendőnek, hogy a térbeliség legfontosabb ismérvei, a korlátozottság, a határok éppen olyan fontos és természetes velejárói a hálózatos világnak, mint a másíknak, a „valóságosnak”. Ennek a koncepciónak a hívei

az „előállításában” persze nem kis szerepet játszik a társadalmakban élő (és egyre több IKT-eszközzel körülvett, azokat minden élethelyzetben használó) emberek sokasága.

³⁰ A tétek nagyságát mutatja az eddigi legnagyobb méretű adatlopás, amikor 2013-ban a Yahoo cég 3 milliárd felhasználójának személyes adatai (telefonszámoktól születési adatokon át rengeteg információ) kerültek illetéktelen adattolvajok kezébe. *Yahoo Says All 3 Billion Accounts Hacked in 2013 Data Theft*. 2017.

³¹ Shaun Riordan: *Cyberdiplomacy. Managing Security and Governance Online*. Cambridge, Polity Press, 2019 az internetszabadság problematikájának legkitűnőbb bemutatását tartalmazza, miközben a kibertér diplomáciai napirendjének egyéb pontjait is például foglalja össze.

³² Ayers jó összefoglalóját adja a kiberzsuverenitás általános vetületeinek, hangsúlyosan a geopolitikai jellegre ügyelve. Lásd Cynthia Ayers: *Rethinking Sovereignty in the Context of Cyberspace*. Carlisle, US Army War College, 2015.

³³ Justin Sherman: *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?* 2019.

a kibertér alapos és aprólékos szabályozottságáért munkálkodnak a nemzetközi egyeztető fórumokon és formációkban is. A szakemberek úgy szoktak fogalmazni, hogy – nagy vonalakban persze – a liberális demokráciák képviselik a netsemlegesség elvét, és az autoriter rendszerű államok szorgalmazzák a szuverenitás elvének kiterjesztését a kibervalóságra is. Kétségtelen, hogy a formálódó multipoláris geopolitikai valóságban inkább a feltörekvő (erős regionális vagy globális pozícióra pályázó) országok ragaszkodnak a nemzeti szuverenitás elvének kiterjesztéséhez a digitális terekre is. Oroszország és Kína jellemzően e felfogás legfőbb szószólóinak számítanak, nem csupán elvben, de a nemzetközi kapcsolatok multilaterális fórumainak gyakorlatában is.³⁴ Természetesen az internet erős szabályozásában, korlátokkal történő lehatárolásában felsejlenek a nyilvánvaló hatalmi-politikai szándékok is. Érdemes azonban emlékezni rá: a kiberszuverenitás (ahogy ellentétpárja, a netsemlegesség is) legalább ennyire fontos gazdasági érdek.

A digitális gazdaság legfontosabb éltetője az adatok határokat átszelő, globális áramlása. Ennek az adatfolyamnak óriási a gazdasági, pénzügyi értéke: a McKinsey pénzügyi tanácsadó számításai szerint a digitális gazdaság értéke már jócskán meghaladja a külkereskedelmi forgalomba kerülő hagyományos javak által generált összegeket.³⁵ A növekedés ráadásul folytatódik, és ennél fogva a gazdaság új „olajának” tekintett adatjavak nemzetközi áramlásának szabályozása óriási gazdasági jelentőséggel bír. Az Egyesült Államok az elmúlt időszak nemzetközi kereskedelmi megállapodásai során a határokon átvívelő szabad adatforgalom híveként kötelezte el magát. Amerika mind a csendes-óceáni úgynevezett TPP-egyezményben,³⁶ mind az USA–Mexikó–Kanada közötti kereskedelmi keretmegállapodásban, mind pedig az USA és Japán közötti digitális kereskedelmi egyezményben ragaszkodott annak garantálásához, hogy az adatok szabadon áramolhassanak a határokon át, illetve hogy a helyi adatokat ne legyen kötelező helyi szervereken tárolni.³⁷

³⁴ Yi Shen: *Cyber Sovereignty and the Governance of Global Space. Chinese Political Science Review*, (2016), 1. 81–93.

³⁵ Sam DuPont: *An Open Alliance for Digital Trade*. 2020.

³⁶ Hivatalos nevén Transz-csendes-óceáni Partnerség, angolul Trans-Pacific Partnership.

³⁷ DuPont (2020): i. m. Figyelemre méltó, jelzés erejű mozzanat, hogy a nemzetközi kereskedelempolitikában a korábbi liberális felfogással sok szempontból szakító Trump-kormány alatt sem változott az USA internetszabadságra (az adatok szabad áramlására) vonatkozó prioritása. Ezt az álláspontot Amerika következetesen érvényesíti továbbra is, például a Világkereskedelmi Szervezetben (WTO) folyó multilaterális tárgyalásokon.

Ezzel a megközelítéssel élesen szemben áll az Egyesült Államokkal egyre inkább minden fronton erőteljes rivalizálásba kezdő Kína álláspontja. A WTO-ban folyó digitális kereskedelempolitikai tárgyalásokon egyértelműen azt a szempontot igyekszik érvényesíteni, hogy az egyes államok korlátozhatók a határaikon átfolyó adatáramlást, megsűrűsítsék az internetes forgalmat, illetve jogukban álljon egyes külföldi digitális tartalmakat blokkolni államhatáraikon belül. Ez az egyes szakemberek megfogalmazásában „kiber vesztfáliai” álláspont³⁸ tükröződik a (Kínán belüli internetet a külvilágról leválasztani képes) úgynevezett „Nagy Kínai Tűzfal” működtetésén, illetve a helyben keletkezett adatok helyi szervereken való tárolását előíró kínai jogszabályokban is. Hasonló pozíciót képvisel ebben a kérdésben Oroszország is: a globális internetről leválaszthatóan működő saját hálózat fejlesztése és próbaüzeme (akárcsak az egyes helyi adatok helyi tárolását előíró törvényei) világosan utalnak a kiber szuverenista álláspont melletti elkötelezettségére.³⁹ A nemzetközi viszonyok fokozatos átrendeződésének egyik jeleként az elmúlt évben több ország (Irán, Vietnám, Kazahsztán, Indonézia) is felzárkózott az ENSZ-ben a kínai és orosz kiber szuverenista javaslatok mögé, miközben más országok is (például a korábban a szabad adatáramlás mellett elkötelezett Japán, vagy különösen India) keresik a módját az adatfolyamok hatékony igazgatásának, kontrollálásának.⁴⁰

³⁸ Chris Demchak – Peter Dombrowski: Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Relations*, (2013–2014). 29–38. A „Vesztfália” szó (ami néha az angolszász írásmód hatását tükröző Weszfália formában is előfordul) gyökere a 17. század nagy európai békekonstrukciójáig nyúlik vissza. A harmincéves háborút lezáró nemzetközi szerződés teremtette meg a nemzetközi kapcsolatok modern szuverenitásfogalmát. Manapság az erős nemzetállami lét elsőségét hangsúlyozó külpolitikai-hatalmi felfogás elnevezésére használatos a vesztfáliai jelző.

³⁹ Sherman (2019): i. m.

⁴⁰ Sherman (2019): i. m. A téma európai uniós megközelítéséhez, és így a formálódó multipoláris rend egyik potenciális pillérének álláspontjához érdemes kézbe venni: Megan Dee: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO*. London, Palgrave MacMillan, 2015. Ugyanakkor megkerülhetetlenül fontos ebben a témában is Riordan (2019): i. m. Fontos észrevételeket tartalmaz az európai erőközpontok (EU) pozíciójáról a befolyásos kutatóműhely, az European Council on Foreign Relations projektje. Stefan Scesanto: *Europe's Digital Power: From Geo-economics to Cybersecurity*. London, European Council on Foreign Relations, 2017.

*Nyílt adatok és adatvédelem: az adatgazdaság alapjai*⁴¹

Az új gazdaságot életető virtuális nyersanyag, az adat egy másik (bár az előző polémiához természetesen több szálon is kapcsolódó) összefüggésben is vitákat, egymással ellentétes koncepciókat, sőt filozófiákat generál a 21. századi kiber-gazdaságban. Ezt a dilemmát úgy lehetne megfogalmazni: az adatok nyíltsága, transzparenciája a fontosabb, vagy inkább az adatok (különösen a személyes adatok) védelme legyen-e a digitális gazdaság vezérlőelve? A digitális gazdaságban működő cégek folyamatosan „vadásznak” az újabb és újabb adattömegekre. Különösen érvényes ez (mint később még látni fogjuk) a mesterségesintelligencia-fejlesztésekre, -alkalmazásokra épülő új iparágakban, amelyek az adattömegek nélkül gyakorlatilag nem is létezhetnek.

Nyílt adatnak azokat nevezhetjük, amelyek szabadon, megkötések nélkül és bárki számára hozzáférhetőek („elvihetők”, felhasználhatók, továbbadhatók), és mint ilyenek gazdasági értékteremtés céljára (magyarul üzleti célokra) is felhasználhatók.⁴² Fontos azt is látni: ahhoz, hogy az adat nyílt legyen, tehát – nemcsak elvben, de ténylegesen is – szabadon hozzáférhető és felhasználható legyen, ahhoz megfelelő formátumban és adatstruktúrában kell lennie. A nyílt adatokat (azok körét, felhasználhatóságát) általában jogszabály írja körül, és jellemző módon a közszférában keletkező (illetve a közszféra szervezetei és intézményei által birtokolt, tárolt, használt) adatokat öleli fel.⁴³ A nyílt adatok körébe tartoznak például az időjárási adatok, a kataszteri (ingatlanügyi) információk, műholdas felvételek, közműtérképek. Ezek használata a gazdasági élet szereplőinek döntési tevékenységét segítheti. Természetesen az adatok újrahazsnosításában (továbbadásában) is jelentős gazdasági értékteremtési potenciál rejlik.⁴⁴

⁴¹ A rendkívül fontos kiberszabályozási témakör korszerű összefoglalóját mutatja be Dário Moura Vicente – Sofia de Vasconcelos Casimiro: *Data Protection in the Internet*. Cham, Springer Nature, 2020.

⁴² Yannis Charalabidis: *The World of Open Data. Concepts, Tools and Experiences*. Cham, Springer Nature, 2018 a téma jó átfogó ismertetését adja, beleértve a nyílt közadatok kérdéskörét is. Bart Custers et al.: *EU Personal Data Protection in Policy and Practice*. Berlin, Springer, 2019 viszont az érem másik oldalát, az adatvédelem koncepcióját járja körül, különös tekintettel az EU gyakorlatára.

⁴³ *Open Government Data Report*. 2018.

⁴⁴ A McKinsey pénzügyi tanácsadó cég tanulmányának becslése szerint a kormányok által szabadon hozzáférhetővé tett, nyílt adatkészletek éves szinten és globálisan mintegy 3 billió dollárnyi új értéket teremthetnek a gazdaság néhány kulcsszektorában, elsősorban az oktatásban,

Az adatok szabad, korlátok nélküli felhasználásához fűződő, erős gazdasági érdekekkel szemben áll ugyanakkor egy másik érdek is, amely az adatok védeltségét, hozzáférhetőségének, mások által történő felhasználhatóságának erős korlátokat szabna. Ez az adatvédelem elsősorban a személyes adatok körét érinti. Az adatok védelmét szintén jogszabály rögzíti, és fontos megjegyezni, hogy ezen a téren az Európai Unió különösen élen jár (a mára közismertté váló, széles körben alkalmazott GDPR-szabályozás kidolgozásával).⁴⁵ Az adatvédelmi jogszabályok rögzítik azokat az elveket és körülményeket, feltételeket, amelyeket az adatok begyűjtőinek, tárolóinak és felhasználóinak szem előtt kell tartaniuk.⁴⁶

Látható tendenciaként jelentkezik, hogy a mesterségesintelligencia-technológiák széles körű elterjedésével (például az arcfelismerő vagy más bionikus azonosító rendszerek tömeges alkalmazásával) az adatvédelem kérdése a korábinál is hangsúlyosabbá válik. Üzleti, biztonsági szempontok és elvek ütköznek itt etikai, személyiségi jogi kívánalmakkal.

Államok és magánszereplők (governance-modellek)

A nemzetközi kiberbiztonsági rendszer, ahogy egyébként maga az egész digitális ökoszisztéma, a kibetér geopolitikai és geoökonómiai rendszere is képlékeny, alakulóban levő formáció. Szabályozó és működtető elveinek, normarendszerének kimunkálásánál (ahogy azt az előző két alfejezetben jól láthattuk) jelentősen eltérő szemléletek, különböző érdekek, egymásnak ellentmondó törekvések munkálkodnak. A kibetér szabályozó és irányító elképzelésekben is két jelentős megközelítés tapintható. Az egyik a kibetér „kormányzását” alapvetően a szuverén államok hatáskörébe utalná, és döntően a nemzetközi jog már létező

a közlekedésben és az egészségügyben. *Open Data: Unlocking Innovation and Performance with Liquid Information. McKinsey Global Institute Report. 2013.*

⁴⁵ Az Általános Adatvédelmi Szabályozás (General Data Protection Regulation) 2018-ban lépett életbe az EU tagállamaiban. Normatív szerepét jól mutatja, hogy az unión kívüli gazdasági szereplők is csatlakoztak az alkalmazásához. A GDPR jelentős előrelépést jelentett az adatok védelme terén az EU korábbi, 1998-ban életbe léptetett adatvédelmi szabályzatához képest.

⁴⁶ Jellemzően például az adatok begyűjtőinek felelősnek (elszámoltathatónak) kell lennie az adatok „tulajdonosaival” szemben. Az adatok begyűjtése csakis jogszerűen történhet. A begyűjtött adatok köre nem lehet korlátlan, csak indokolt adatkörre és adatmennyiségre vonatkozhat. Az adatok tárolása is csak jogszabályban meghatározott, korlátozott időtartamig lehetséges. A begyűjtött adatok tárolása és felhasználása biztonságos körülmények között kell hogy történjék.

szabályrendszereit igazítaná az új geopolitikai, geoökonómiai térrendszer megváltozott valóságához, és alkalmazná a digitális világában is.⁴⁷ Illetve létezik egy másik felfogás, amelyik a magángazdaság szereplőit, elsősorban a nagy internetes cégeket, technológiai globális vállalatokat is bevonná a normatív szabályozásba, a digitális geoökonómiai komplexum igazgatásába. Az előbbi álláspont legfajtsúlyosabb szószólója a nemzetközi porondon az Egyesült Államok, amely globálisan (és önkéntesen) elfogadott normarendszerrel biztosítaná a kibertér szabályozott működését, és amely a kibertérség irányításába bevonná a magángazdaság meghatározó szereplőit is. A másik elképzelést elsősorban Oroszország és Kína képviseli a vitákban, amelyek multilaterális szerződésrendszerrel, és így értelemszerűen csak szuverén szereplők (államok) által kormányozva garantálnák a kibervilág biztonságát, kiszámítható működtetését.⁴⁸

Érdemes egy további pillantást vetnünk arra a megközelítésre, illetve törekvésre, amely a kibertér nemzetközi szabályrendszerének kimunkálásába kezdetől bevonná a magáncégek képviselőit is. Furcsának tűnhet, de ezt a gondolatot mindkét részről (nagyvállalati oldalról, illetve a szuverén állami aktorok térfeléről is) jelentős erők támogatják. Láttuk egy kicsit feljebb, hogy a technológiai cégek milyen óriási értéktérmetítő potenciállal rendelkeznek. A méretek összehasonlító érzékeltetésére érdemes rámutatni: a nagy internetes platformüzemeltető globális vállalatokat tömörítő cécsoport együttes értéke mintegy 7 billió dollárra rüg, ami jelentősen meghaladja a világ bármely országának a GDP-jét, kivéve természetesen az USA-t és a Kínai Népköztársaságot.⁴⁹ A Rettegett Ötöknek is nevezett óriásvállalati kör teljesítményadatai egyenként is több, mint imponálóak: az élen természetesen a Microsoft áll az 1000 milliárd dollárt éppen meghaladó piaci kapitalizációs⁵⁰ értékkel, de nem sokkal marad el tőle az Amazon (888 milliárd dollár), az Apple (875 milliárd), a Google (741 milliárd) és a Facebook (496 milliárd dollár) piaci értéke.⁵¹ A nemzetközi erőviszonyok további érzékeltetésére

⁴⁷ Stadnik Ilona: *What Is an International Cyber Regime and How We Can Achieve It?* *Masaryk University Journal of Law and Technology*, 11. (2017), 1. 129–154. 146. és Sash Jayawardane: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance*. The Hague, The Hague Institute for Global Justice, 2015. 5.

⁴⁸ Stadnik (2017): i. m. 134.

⁴⁹ *Data Governance. Part I. Emerging Data Governance Practices*. 2020.

⁵⁰ Egy vállalat piaci kapitalizációja olyan pillanatnyi piaci értékösszeget mutat, amelyet a piac (a befektetők) az adott időpontban a cégnek tulajdonít. Lényegében a vállalat részvényei számának és azok pillanatnyi piaci árfolyamának (ez folyamatosan változhat!) a szorzatával adható meg.

⁵¹ Samuele Dominioni: *Digital Economic Powers and Digital Political Rulers*. 2019. október 17.

egyébként azt sem haszontalan megjegyezni: az első tíz ilyen technológiai óriásvállalat között két kínai található, a bolygónk alsó végében.⁵² Az ebben a roppant gazdasági erőben rejlő hatalmi realitás sok állam képviselői számára is azt diktálja, hogy célszerűbb ezeket a gigantikus szereplőket bevonni a játékszabályok kialakításába, a békés ügymenet fenntartásába. Ennek a felismerésnek válfajaként jelent meg a nemzetközi kiberdiplomáciai porondon egy merőben új tisztség és munkakör: a technonagykövet szerepköre. Első képviselője Casper Klynge hivatásos dán diplomata lett, aki országát szabályos nagyköveti meghatalmazással képviselte az USA-ban és Kínában is.⁵³ Azonban nem az említett országokhoz akkreditálva kezdte meg munkáját, hanem a világ vezető technológiai cégeihez „delegálva”. Elsőként ennek megfelelően az amerikai Szilícium-völgyben épített ki képviseletet 2017-ben, majd hamarosan Pekingben is megnyitotta regionális irodáját Dánia technonagykövete.⁵⁴ Működésének deklarált célja az, hogy a (digitalizációban egyébként korántsem lebecsülendő teljesítményt mutató) skandináv ország közvetlen párbeszédet kezdhesen az internetgazdaság meghatározó szereplőivel, méghozzá éppen a nemzetközi szabályozási keretrendszer előmozdítására. Az állam–cég közvetlen együttműködés kiemelt tématerületei egyébként a kiberbiztonság, illetve a digitális gazdaság etikai kérdései is. A várakozás az, hogy ilyen új formájú „népi diplomáciai” szintek kiépítésével Dánia a technológiai fejlesztések élvonalába kerülhessen.

Mesterséges intelligencia: biztonság és gazdaság újraértelmezése a kibertérben

„Aki a mesterségesintelligencia-kutatásokban az élre kerül – az uralja majd az egész világot.” Vlagyimir Putyin orosz elnök két éve elhangzott idézetét nyugodt szívvel választhattuk volna jelen tanulmány mottójának.⁵⁵ Az innovációkutatók a nagy társadalmi átalakítások motorjaként úgynevezett „általános célú technológiákat” (GPT) azonosítanak, amit persze talán pontosabb volna

⁵² Dominion (2019): i. m. A vezető technológiai nagyhatalmak között találjuk 402 milliárd dolláros piaci kapitalizációval a kínai Alibaba céget, illetve a szintén kínai Tencetet, 398 milliárd dollárral.

⁵³ Nurtulzah Rohaidi: *Exclusive: Meet the World's first Tech Ambassador*. 2017.

⁵⁴ *The World's First Ambassador to the Tech Industry*. 2019.

⁵⁵ Meyer (2017): i. m.

„átfogó hatókörűnek” neveznünk. Ezek azok a technológiai újítások, amelyek (az általuk generált további részinnovációk sorával együtt) meghatározó változásokat idéznek elő a köznapi emberi életben és az üzleti-termelői világban egyaránt.⁵⁶ Ebben a körben az elmúlt kétszáz év nagy technológiai változtatásai négy egymást követő hullámban érkeztek: elsőnek a gőzgép, majd az elektromosság, illetve az informatika. A negyedik hullám hátán most érkezik éppen a mesterséges intelligencia.

Az innovációban rejlő geopolitikai és geoökonómiai⁵⁷ potenciál – amelynek érzékeltetésére a híres amerikai politikus és geopolitikai gondolkodó, Zbigniew Brzezinski sakktábla-metaforáját⁵⁸ emeltük ide – természetesen nem csupán az orosz vezető számára nyilvánvaló. Igazi technológiai versenyfutásnak lehetünk tanúi, amelyben egyébként Oroszország, szakértők véleménye szerint, a vezető helyről aligha álmodhat komolyan. A legesélyesebb versenyzőnek most többnyire Kínát tekintik: a 2015-ben bejelentett Made in China program 1,36 billió dolláros fejlesztési forrásai, amelyek zöme MI-kutatásokra és fejlesztésekre irányul majd, nagyságrenddel haladják meg a többi versenyző állam célzott fejlesztési befektetéseit. Ugyanakkor sokat számíthat a vetélkedésben az USA vállalkozás- és innovációbarátabb környezete, vagy az EU perspektivikusabb jogi szabályozó közegei. És a pénzügyi erőben tetten érhető hátrányos helyzet ellenére komoly versenyben van még az MI-forradalom kibontakoztatásában Japán, Nagy-Britannia, Franciaország, Németország, továbbá a már említett Oroszország és Kanada.

A verseny tehát éles, a tempó – ebben mindenki egyetért – exponenciálisan növekvő. Az elkövetkező évtized várhatóan döntő lesz ebben az új technológiai forradalomban. És ha igaz az, hogy a kibertér a geopolitikai érdekérvényesítés új, sőt meghatározó dimenziója, az egymással szemben nemzeti érdekeik érvényesítéséért küzdő szereplők 21. századi sakktáblája, akkor ezen a véresen komoly játékmezőn a mesterséges intelligencia lesz a legfontosabb bábu, a kiber sakktáblák királynöje.

A digitális diplomácia, a kiberdiplomácia szakértői nagyjából egyetértenek abban, hogy a mesterséges intelligencia két alapvető – és egymástól

⁵⁶ Indermit Gill: *Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100*. 2020.

⁵⁷ Filippov (2019): i. m. kitűnő, friss összegzése a digitális gazdaság problématerületeinek. Hangsúlyosan jelennek meg nála a mesterséges intelligencia alkalmazások nyomán támadó kibergeopolitikai és kiberbiztonsági kérdések is.

⁵⁸ Zbigniew Brzezinski: *A nagy sakktábla*. Budapest, Európa, 1999.

eltérő – módon kapcsolódhat, kapcsolódik a külügyi igazgatási struktúrák és különösen a diplomáciai szervezetek működéséhez.⁵⁹ Érdemes felidézni, hogy hasonló a helyzet az átfogóbb „digitalizáció” fogalom és a külügyek, illetve diplomácia kapcsolódási lehetőségeinél. A digitalizáció egyfelől tématerülete lehet a diplomáciának: ezt, az online terek, működések és szereplők szabályozásával kapcsolatos diplomáciai, államközi tevékenységet nevezzük mi „kiberdiplomáciának”. Másfelől a digitalizáció új eszközöket biztosíthat a nemzeti külpolitikai érdekek érvényesítéséért felelős diplomáciai szervezetek hatékony és korszerű működéséhez. Ezt a technologizált eszközparkot és működést nevezzük „digitális diplomáciának”. Hasonló kettősséget találunk a digitalizáció szélesebb témakörén belüli, meghatározó technológiai fejlesztések, a mesterséges intelligencia külügyi kapcsolódásainak esetében is.

Mesterséges intelligencia: fogalmi alapok

Elsőként is fontos leszögezni, hogy a „mesterséges intelligencia” nem egyetlen technológiát jelöl, hanem sokkal inkább a komputertudomány egy jellemzően interdiszciplináris kutatási területét, illetve az ezekhez kapcsolódóan fejlesztett technológiákat és alkalmazásokat. Az MI fókuszában az emberre jellemző intelligens tevékenységek (folyamatok) számítógépes rendszerek általi szimulációját értjük.⁶⁰ E tevékenységek felölelik mindenekelőtt az emberi tanulás képességét (tehát információk és az információk használatához szükséges szabályok megszerzésének képességét); felölelik továbbá az emberi érvelés képességét (tehát azt, hogy a szabályokra támaszkodva következtetéseket tud levonni); és különösen fontos képességként öleli fel az önkorrekció képességét.

Érdemes kiemelni azt is: a mesterséges intelligencia szorosan kapcsolódik a big data fogalmához. A big data nagymennyiségű, rendkívüli változatosságú/összetettséggű és gyorsan változó adattömeget takar. Ezek az adattömegek

⁵⁹ A fogalmi rendszer olyan kulcselemeinek, mint a „digitális diplomácia”, illetve a „kiberdiplomácia” tisztázásához, illetve az átfogó digitális diplomáciai keretrendszer elemeivel kapcsolatos különbségtételekhez vö. Nyáry (2020): i. m.

⁶⁰ A mesterséges intelligencia áttekintéséhez jó kiindulás pontot ad a téma egyik legkiválóbb magyar kutatójának kötete: Futó Iván: *Mesterséges intelligencia*. Budapest, Aula, 1999. A mérnöki-informatikusi előképzettséggel nem rendelkező humán szakembereknek, olvasóknak különösen nagy segítséget jelenthet egy friss angol nyelvű monográfia: Tom Taulli: *Artificial Intelligence Basics. A Non-Technical Introduction*. Monrovia, Apress, 2019.

a hagyományos eszközökkel (például adatbázis-kezelőkkel) nem kezelhetők már. Feldolgozásukhoz éppen az MI-technológiák nyújtanak segítséget. Ugyanakkor elmondható az is: az MI egyik fontos technológiáját jelentő gépi tanulási eljárások nem képzelhetők el olyan (számottevő, többnyire a big data fogalomkörébe sorolható) adattömeg nélkül, amely az algoritmusok tréningezésére szolgál.

Fontos megemlíteni a mesterségesintelligencia-technológiák klasszifikációját, azaz főbb csoportjait vagy alosztályait. A diplomácia működési területén jelenleg alkalmazott okosmegoldások kapcsán szokás néha megemlíteni, hogy azok még aligha tekinthetők „igazi” mesterségesintelligencia-technológiáknak; valójában csak azokhoz hasonló, ám valójában inkább csak „pszeudó-MI”-technológiáknak nevezhetjük azokat.⁶¹ Ez az óvatos megközelítés annak a tényleges jelenségnek egyfajta ellenhatása, amely a modern korban (különösen a nem szakmai közbeszédben), alapvetően divatmegfontolásból használ megalapozatlan fogalmakat.

Ténylegesen az MI-technológiákat szokás úgynevezett általános képességű mesterséges intelligencia, más néven „erős MI” kategóriába, illetve szűk alkalmazási képességű mesterséges intelligencia, más megnevezéssel „gyenge MI” kategóriába sorolni. A „gyenge MI” lényegében egyetlen célfeladat elvégzésére tervezett és betanított MI-technológiát takar. Jellemző példája a közönségkapcsolati rendszerekben alkalmazott beszélgetőrobot. Természetesen igaz, hogy ma még a diplomáciai feladatkörökben is többnyire ilyen MI-alkalmazásokat találunk. Akad azonban – igaz, egyelőre kísérleti jelleggel – példa az „erős MI” külső célú alkalmazására is: a lejjebb felvillantott esettanulmányoknál több példát is bemutatunk majd rá. Ezeknél a technológiáknál részben vagy egészben sikerül immár szimulálni az általános hatókörű emberi kognitív képességeket (tehát például egy addig ismeretlen feladat eredményes megoldásához szükséges „intelligenciát”).

*Az MI a diplomáciai szervezetek eszköztárában*⁶²

A bevezető részekben szó volt a geopolitikát várhatóan átformáló fejleményekről. Ugyanakkor a mesterségesintelligencia-technológiák nem csupán a nemzetközi kapcsolatok környezetét, az államok közötti vetélkedés geopolitikai sakkjátláját

⁶¹ Nyáry (2020): i. m.

⁶² *Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy*. 2019.

rajzolhatják át teljesen, de az államközi érdekérvényesítés békés intézményrendszerének tekinthető diplomácia eszköztárát is. Az adatok már ma is a diplomáciai háttérműveletek éltető alapanyagát szolgáltatják. A big data-ra alapozott eszközök, részben már MI-alkalmazások a digitális diplomácia eszközrendszerének gerincét képezik ma is az információgyűjtéstől és feldolgozástól kezdve a szoftverrel támogatott külügyi döntéshozatalig sok területen. És a nyersanyag, az adat szédítő tempóban növekszik tovább, a nap minden percében. Ami – ha figyelembe vesszük, hogy egyetlen év alatt mintegy 370 millióval nőtt az internethasználók száma – nem is meglepő. A mesterséges intelligencia tehát egyfelől eszközként kapcsolódik a külügyi szervezetekhez, mindenekelőtt (de, mint az esettanulmányokból látni fogjuk, nem kizárólagosan) a politika végrehajtásáért felelős diplomáciai szervezetekhez és működésekhez.⁶³

A tájékozódás és tájékoztatás a diplomáciai munka alapvető funkciója volt és maradt. Jelentősége mindkét irányú információáramoltatásnak növekedett, noha természetesen – a közösségi platformokon zajló közdiplomácia népszerűségének szárnyalásával – elsősorban a tájékoztatás jut róla az eszünkbe. Az MI-projektek jó része ugyanakkor a diplomáciai információszerző, rendszerező, elemző, prezentáló munkát igyekszik új minőségi szintre emelni. Közben a tájékoztatáshoz kapcsolódóan is egyre több az MI-kezdemenyezés, elsősorban az álhírprobléma kezelésére.⁶⁴

Az adattudomány, a mesterséges intelligencia, a különféle modellezések alkalmazásának érdekes példáját adja a brit külügyi szervezet fejlesztése. Az általuk kialakított MI-alapú informatikai eszközrendszer több százezer, különböző nyelvű információs forrást képes automatikusan figyelni, angolra fordítani és valós időben megjeleníteni egy központi felhasználói felületen. Korábban a diplomatáknak rengeteg időt kellett fordítaniuk a helyi hírforrások olvasására. Most az így szerzett információkat az online források tömegéből beszerezhető értesülésekkel lehet számottevően kiegészíteni. A „gyorsreagálási” külügyi csoportok (például válságok idején) rövid határidő alatt készülhetnek fel olyan információtömegből, amelynek megszerzésére korábban egyszerűen nem volt

⁶³ A mesterséges intelligencia külügyi, diplomáciai alkalmazásaiban rejlő lehetőségeket és kihívásokat a digitális diplomácia egyik legfigyelemreméltóbb európai kutatóműhelye, a genfi székhelyű DiploFoundation tanulmányozza önálló programként immár két éve. *Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy*. 2019.

⁶⁴ A tájékoztatási funkcióhoz kapcsolódó MI-alapú alkalmazásra példának lásd a Brit Külügyminisztérium Nyílt Forrású Osztályát (OUSU). Hasonlóan jó bepillantást enged a legújabb adat alapú külügyi fejlesztések irányába a Svéd Intézet közösségi média hírszerző funkciója.

lehetőség. Az adatok hasznosulásához azonban nélkülözhetetlen az is, hogy azokat a maguk „emberi kontextusába” helyezzék. Ezért foglalkoztatnak viselkedéstudományban járatos szakembereket is. Az ő feladatuk, hogy felfedezzék az adatokból kirajzolódó tendenciákat, rámutassanak a mögöttük megbúvó emberi viselkedésekre. A csoport egyik fontos profilja ugyanis az „extrém megnyilvánulások” figyelése.⁶⁵

A konzuli feladatok, a külügyi szervezet par excellence igazgatási típusú feladatai zömében nem egyedi, típusproblémák kezelését igénylik, viszont sokszor rövid határidővel, és néha jelentős távolságokból is. A konzuli ügyintézés éppen ezért ideális terepet kínál az egyszerű „gyenge MI”-technológiák alkalmazására, a hatékonyság számottevő növelése érdekében. A legjellemzőbb és ma már széles körben elterjedt ilyen MI-technológiákra támaszkodó alkalmazások a konzuli tevékenységhez kapcsolódó chatbotok. A konzuli beszélgetőrobotok elsősorban utazással kapcsolatban segítik az ügyfelet, másrészt a tipikusan külföldön előforduló vészhelyzetekkel kapcsolatban biztosítanak gyors, hatékony tájékoztatást – ráadásul a nap minden szakában.⁶⁶

A diplomáciai szervezetek működésének – ahogy a diplomata munkának is – máig egyik legfontosabb, meghatározó feladata, funkciója maradt a nemzetközi (két- vagy többoldali) tárgyalások folytatása. E már-már művészetnek számító munkafolyamat technológiai támogatására fejlesztették ki a „Debatör” projektet, amelynek algoritmusai beszélgető interfészen keresztül vitába képes szállni emberi partnerekkel. A fejlesztés mögött álló izraeli külügyi szakemberek a diplomácia máig legfontosabb funkciója, a tárgyalások támogatásának új eszközét remélik ettől a speciális MI-fejlesztéstől.⁶⁷

A kereskedelmi attaséi hálózatokkal, illetve a külképviselektől sokszor elkülönülve működő, de azok általános irányítása alatt maradó kereskedelmi képviselőkkel kapcsolatos megnövekedett elvárásoknak azonban az emberi és tárgyi erőforrásokban többnyire szűkölködő szervezetek mind nehezebben képesek megfelelni. Nem véletlen, hogy a diplomáciai tevékenység e speciális szekciójában is nagy reményeket fűznek az IKT-technológiák, és specifikusan az MI-fejlesztésekben rejlő „erősokszorozó” lehetőségekhez. Erre példa

⁶⁵ Nyáry (2020): i. m. 11., továbbá *Exclusive: Meet the UK's „Data Diplomat”* (é. n.).

⁶⁶ Nyáry (2020): i. m. 9.

⁶⁷ Nyáry (2020): i. m. 12., továbbá *Inside Project Debater Speech by Crowd* (é. n.).

a Portugál Külügyminisztérium égisze alatt kifejlesztett „Portugal Exporta” portál, számos MI-vel támogatott funkcióval segítve az ország külkereskedelmét.⁶⁸

Utójára hagytuk az MI-technológiákra támaszkodó „diplomáciai” fejlesztések legérdekesebbikét. Merthogy nem a külpolitika végrehajtásáért felelős diplomáciához (tehát a taktikai szinthez) kapcsolódik, hanem magához a nemzeti külpolitika formálásához, a külügyi stratégiaalkotáshoz. A Kínai Tudományos Akadémia által fejlesztett, MI-alapú külpolitikai döntéstámogató rendszer korai változatát már használja is a feltörekvő ázsiai nagyhatalom külügyi apparátusa. A szoftver óriási adattömeget elemez, a diplomáciai koktélpártik pletykáitól a nemzetbiztonsági stratégiákig. Ha a külpolitika alakítói egy komplex helyzeten belüli konkrét külkapcsolati cél eléréséhez szükséges döntéseket latolgatják, akkor a szoftver villámgyorsan több, nagyon pontos döntési alternatívát rajzol fel nekik.⁶⁹

Kiberdiplomácia az MI nemzetközi szabályozásában

A mesterséges intelligencia ugyanakkor a diplomáciai tevékenységek új téma-területeként is jelentkezik. Azaz: nemcsak a mesterségesintelligencia-technológia segíti a diplomácia működését, de a diplomácia is támogatja működésével a mesterséges intelligencia térhódítását. Láttuk, hogy ennek az új technológiának mekkora jelentőséget tulajdonítanak a modern geopolitikai kapcsolatrendszerekben. Nem meglepő, hogy a mesterséges intelligencia, annak technológiai, alkalmazási, személyes adatvédelmi, sőt etikai vonatkozásai erősen foglalkoztatják a nemzetközi közvéleményt. Ebből következően az ezeknek a – sok szempontból újszerű, analógiák és megszokott fogódzkodók nélküli – helyzeteknek a kezelésére szolgáló nemzetközi szabályozások kidolgozására növekszik az igény. Már most látható, hogy az MI-tématerület a diplomácia, és ezen belül is az úgynevezett multilaterális kapcsolatok egyik legfontosabbjaként kezd szerepelni. Ezen a területen különösen aktív az Európai Unió, de az ENSZ is fontos kezdeményezésekkel, célzott munkacsoportokkal és más nemzetközi fórumokkal törekszik e nagy hatású geopolitikai vonatkozású technológia nemzetközi szabályrendszerének kidolgozására.

⁶⁸ Nyáry (2020): i. m. 37.

⁶⁹ Nyáry (2020): i. m. 37.

A mesterségesintelligencia-kutatások, fejlesztések és alkalmazások körülményeinek átfogó szabályozása minden kétséget kizárólag ma az egyik legégetőbb feladat. A technológiában rejlő elképesztő potenciálok, és így a várható fejlődés üteme és kiterjedése nélkülözhetetlenné teszi a szabályrendszerek kidolgozását. Éppen ezért az elkövetkező időszakban vélhetően ez a tématerület áll majd a kiberdiplomatak figyelmének fókuszában. Ugyanakkor a mesterséges intelligencia szabályozására, illetve a kapcsolódó szakpolitikákra vonatkozó nemzetközi jogi környezet még maga is csupán kialakulóban van.

Az MI-szabályozás részben a technikai, részben a gazdasági, részben pedig a társadalmi alkalmazási (etikai) aspektusokra fókuszál. Maga a jogi szabálykörnyezet kialakítása jelenleg az alábbi fő témákkal foglalkozik elsősorban: autonóm intelligens rendszerek, az MI-rendszerek felelőssége és számonkérhetősége, valamint a személyiségi jogi és biztonságossági kérdések.⁷⁰ A szabályozás nemzetközi kereteinek megteremtése a 2010-es évtized második felétől került a multilaterális fórumok érdeklődési körébe. 2018-ban közös kanadai–francia kezdeményezésre merült fel az elképzelés, hogy (a klímaváltozással foglalkozó nemzetközi panel példájára) a G7-es csoport égisze alatt induljon el egy Mesterséges Intelligencia Nemzetközi Panel az új technológiai fejlesztési terület lehetséges globális kihatásainak tanulmányozására. 2019 tavaszán elfogadták az OECD *Mesterséges intelligencia ajánlásait*, majd néhány hónapra rá a G20-as csoport *Mesterséges intelligencia alapelveit*. Még szintén 2019-ben a Világgazdasági Fórum is kibocsátott egy útmutatót a kormányzati MI-beszerzések támogatására.⁷¹

A világ vezető multilaterális tömörüléseihez hasonlóan az EU is a mesterségesintelligencia-szabályozás előmozdítása mellett kötelezte el magát az évtized utolsó éveiben. 2018 nyarán a Bizottság független Magas Szintű Szakértői Csoportot állított fel a mesterséges intelligencia kérdéseinek – elsősorban a technológia megbízhatóságának – tanulmányozására.⁷² Az MI-szabályozás témájában mérföldkönek tekinthető 2020 februárja, amikor az EU Bizottság publikálta a *Mesterséges intelligencia fehér könyvét*.⁷³ A dokumentum azonosította

⁷⁰ Tom Wheeler: *History's Message about Regulating AI*. 2019.

⁷¹ France and Canada Create New Expert International Panel on Artificial Intelligence (2018) és OECD Principles on AI (2019), valamint G20 Human-Centered AI Principles (2019), továbbá World Economic Forum AI Government Procurement Guidelines (2019).

⁷² Buddle Findlay: *Artificial Intelligence and the Regulatory Landscape*. 2020.

⁷³ White Paper on Artificial Intelligence. A European Approach to Excellence and Trust. 2020.

a mesterségesintelligencia-fejlesztések és -alkalmazások kapcsán felmerülő legfontosabb kockázati tényezőket: az alapvető jogok sérülhetősége, az adatokhoz fűződő személyiségi jogok sérülhetősége, a biztonsággal és a hatékony működéssel kapcsolatos problémák, valamint a felelősségrevonhatóság kérdése. A Bizottság úgy határozott, hogy a fejlesztéseknek ebben a relatíve korai fázisában nem bocsát még ki részletes szabályozást a témában, hanem csupán felvázolt egy jogi követelményrendszert, amely értelmében minden jövőbeli keretszabályozásnak garantálnia kell az MI-rendszerek megbízhatóságát, illetve azt, hogy tiszteltben tartják az Európai Unió alapvető elveit és értékeit. A követelményrendszer kitér arra is, hogy a hatályos EU-jog alkalmazandó – technikai tisztázásokat követően – az MI-kérdésekre is.

Kitekintés

A kibertér geoökonómiáját, kiberdiplomáciai témáit és kihívásait és szabályozási törekvéseit bemutatni szándékozó áttekintésünket a nemzetközi szabályozási törekvések ellentmondásaival és ellentéteivel, majd a digitális gazdaságot a várakozások szerint gyökerestül felforgatni készülő mesterséges intelligencia témáival zártuk. Nem haszontalan, ha most zárszóként egy pillanatra mondanánk első részeihez kanyarodunk vissza, oda, ahol az újra megjelenő, majd mind jobban élesedő geoökonómiai szembenállások rendszeréről szóltunk. Esetleg azért is, hogy a két végpontot most mintegy egybeöleljük. A kibertér egyre inkább a hatalom meghatározó dimenziója.⁷⁴ És, ha lettek volna illúzióink, akkor most már kristálytisztán láthatjuk: a gazdaság (a termeléssel és ellátási láncokkal, nemzetközi kereskedelemmel és technológiával) jórészt nemzetbiztonság is – hatalom. Kibertér és digitális gazdaság: egymásba fonódó hatalmi dimenziók tehát. Az egyik jeles kyberszakmai szervezet, az Internet Governance közelmúltban megjelent írása arra figyelmeztet: az Egyesült Államok és Kína között a tavalyi évben elmélyülő, majd mostanra végképp elmérgesedő kereskedelmi háború ma már egyértelműen technológiai konfrontációt takar. A tét nem egy-egy jól jövedelmező fejlesztés vagy versenyelőny, hanem a globális hegemoniában kulcsszerepet kapó kibertér, a geopolitika 5. dimenziójának urálása. Azé a közegé, ahol hamarosan a mesterséges intelligenciával támogatott

⁷⁴ André Barrinha – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs*, 96. (2020), 3. 749–766. 756.

rendszerekre támaszkodva igyekszik majd operálni a támadó és a védekező fél egyaránt. Sokan úgy tartják: ez (is) egy olyan terület, ahol a rendet, biztonságot megőrizni akarók vannak hátrányban. A gépi tanulás ugyanis ma már olyan gyorsan képes megkerülni, lebontani a kibervédelmi rendszereket, amellyel a szokványos védelmi eszközök nem tudnak lépést tartani. A gépi tanulást persze a kibervédelemért felelős szakemberek is csatasorba állítják. Az MI segítségével a fenyegetést jelentő online viselkedési mintákat igyekeznek felderíteni. És, miközben a kiberharcosok a hálózatos térben keresik a megfelelő fegyvert, addig ugyanott keresik a rendezés lehetőségeit mások is. A ma már egyre gyakrabban csak fejlett technológiájú „új hidegháborúként” emlegetett szembenállás ugyanis ösztönzi a kibertér békés rendezésén, kollektív szabályozásán munkálkodó szakembereket, a kiberdiplomátákat is.

Felhasznált irodalom

- Ayers, Cynthia: *Rethinking Sovereignty in the Context of Cyberspace*. Carlisle, US Army War College, 2015.
- Barrinha, André – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs*, 96. (2020), 3. 749–766.
- Brangetto, Pascal – Mari Kert-Saint Aubyn: *Economic Aspects of National Cyber Security Strategies. Project Report*. Tallin, CCDCOE, 2015.
- Brzezinski, Zbigniew: *A nagy sakktabla*. Budapest, Európa, 1999.
- Buchan, Russell: *Cyber Espionage and International Law*. Oxford, Hart, 2019.
- Charalabidis, Yannis: *The World of Open Data. Concepts, Tools and Experiences*. Cham, Springer Nature, 2018.
- Covid-19 Cybercrime Weekly Update*. 2020. Online: www.riskiq.com/blog/analyst/covid19-cybercrime-update/.
- Custers, Bart et al.: *EU Personal Data Protection in Policy and Practice*. Berlin, Springer, 2019.
- Data Governance. Part I. Emerging Data Governance Practices*. 2020. Online: https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map/?utm_source=PostU.
- D' Elia, Danilo: La Guerre économique a l'Ère du Cyberspace. *Hérodote*, (152–153. (2014), 1–2. 240–260.
- Dee, Megan: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO*. London, Palgrave MacMillan, 2015.

- Demchak, Chris – Peter Dombrowski: *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*. *Georgetown Journal of International Relations*, (2013–2014). 29–38.
- Digital Watch Newsletter*. 2020. Issue 50, May 2020.
- Dominioni, Samuele: *Digital Economic Powers and Digital Political Rulers*. 2019. október 17. Online: www.ispionline.it/en/publicazione/digital-economic-powers-and-digital-political-rulers-24187.
- DuPont, Sam: *An Open Alliance for Digital Trade*. 2020. Online: www.csis.org/analysis/open-alliance-digital-trade?utm_source=Members&utm_campaign=aba-3460b2a-EMAIL_CAMPAIGN_2020_01_29_04_21_COPY_01&utm_medium=email&utm_term=0_e842221dc2-aba3460b2a-221725217.
- Exclusive: Meet the UK's „Data Diplomat”* (é. n.). Online: <https://govinsider.asia/innovation/uk-foreign-office-open-source-unit-data-diplomat-graham-nelson/>.
- FBI–CSISA PSA PRC targeting of COVID-19 research organizations* (2020). Online: www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations.
- Filippov, Vladimir M. – Alexander A. Chursin – Julia V. Ragulina – Elena G. Popkova: *The Cyber Economy. Opportunities and Challenges for Artificial Intelligence in the Digital Workplace*. Cham, Springer Nature, 2019.
- Findlay, Biddle: *Artificial Intelligence and the Regulatory Landscape*. 2020. Online: www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716.
- France and Canada create new expert International Panel on Artificial Intelligence* (2018). Online: www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence.
- Futó Iván: *Mesterséges intelligencia*. Budapest, Aula, 1999.
- G20 Human-Centered AI Principles* (2019). Online: www.mofa.go.jp/files/000486596.pdf.
- Gady, Franz-Stefan: *Interview: Robert Ward and Yuka Koshino on Geo-Economics in East Asia*. 2020. Online: <https://thediplomat.com/2020/04/interview-robert-ward-and-yuka-koshino-on-geo-economics-in-east-asia/>.
- Gill, Indermit: *Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100*. 2020. Online: www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/?fbclid=IwAR3UJSDFUG4aFGXpHRDdch76HQu9ZgDIOQXGZo-2t8iVjn-0HIQPNPnD42MM.
- Hakmeh, Joyce: *Cybercrime and the Digital Economy in the GCC Countries*. London, Chatham House, 2017.
- Huang, Keman et al.: *Interactions between Cybersecurity and International Trade: A Systematic Framework*. Cambridge, MIT Sloan, 2018.

- Inside Project Debater Speech by Crowd* (2019). Online: www.linkedin.com/pulse/inside-project-debater-speech-crowd-ibms-effort-extend-rodriguez
- International Trade Regulation and Cybersecurity* (é. n.). Online: www.hoganlovells.com/en/publications/international-trade-regulation-and-cybersecurity.
- Jacobson, Barbara Roseb – Katharina E. Höhne – Jovan Kurbalija: *Data Diplomacy*. Genf, DiploFoundation, 2018.
- Jayawardane, Sash: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance*. The Hague, The Hague Institute for Global Justice, 2015.
- Luttwak, Edward: From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest*, (1990), 20. 17–23.
- Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy*. Geneva, DiploFoundation, 2019.
- Measuring the Digital Economy*. Washington, International Monetary Fund, 2018.
- Meltzer, Joshua: *Cybersecurity, Digital Trade, and Data Flows. Re-Thinking a Role for International Trade Rules*. 2019. Online: www.brookings.edu/research/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/.
- Meyer, David: Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World. *Fortune*, 2017. szeptember 4. Online: <https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/>
- Moisio, Sami: Re-Thinking Geoeconomics: Towards a Political Geography of Economic Geographies. *Geography Compass*, 13. (2019), 10. 1–13.
- Nyáry Gábor: Kiber geopolitika. Mesterséges intelligencia alkalmazások az államigazgatás külpolitikai alrendszerében. *Új Magyar Közigazgatás*, 13. (2020), 1. 32–39.
- OECD Principles on AI* (2019). Online: www.oecd.org/going-digital/ai/principles/.
- Open Data: Unlocking Innovation and Performance with Liquid Information*. McKinsey Global Institute Report (2013). Online: www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.
- Open Government Data Report*. Paris, OECD, 2018.
- Pintő István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája*. 2016/1. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.
- Riordan, Shaun: *Cyberdiplomacy. Managing Security and Governance* Online. Cambridge, Polity Press, 2019.
- Rohaidi, Nurtizah: *Exclusive: Meet the World's first Tech Ambassador*. 2017. Online: <https://govinsider.asia/innovation/danish-tech-ambassador-casper-klynge/>.
- Scesanto, Stefan: *Europe's Digital Power: From Geo-Economics to Cybersecurity*. London, European Council on Foreign Relations, 2017.

- Shen, Yi: Cyber Sovereignty and the Governance of Global Space. *Chinese Political Science Review*, (2016), 1. 81–93.
- Sherman, Justin: *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?* 2017. Online: www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.
- Sherman, Justin: *To Preserve a Global and Open Internet, We Need to Invest in Cyber Diplomacy*. 2018. Online: www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/preserve-global-and-open-internet-we-need-invest-cyber-diplomacy/.
- Significant Cyber Incidents* (2020). Online: www.csis.org/programs/technology-policy-program/significant-cyber-incidents.
- Stadnik Ilona: What is an International Cyber Regime and How We Can Achieve It? *Masaryk University Journal of Law and Technology*, 11. (2017), 1. 129–154.
- Taulli, Tom: *Artificial Intelligence Basics. A Non-Technical Introduction*. Monrovia, Apress, 2019.
- Teoh, Chooi Shi – Ahmad Kamil Mahmood: National Cyber Security Strategies for Digital Economy. *Journal of Theoretical and Applied Information Technology*, 95. (2017), 23. 6510–6522.
- The World's First Ambassador to the Tech Industry* (2019). Online: www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html.
- Vicente, Dário Moura – Sofia de Vasconcelos Casimiro: *Data Protection in the Internet*. Cham, Springer Nature, 2020.
- Wheeler, Tom: *History's Message about Regulating AI*. 2019. Online: www.brookings.edu/research/historys-message-about-regulating-ai.
- White Paper on Artificial Intelligence. A European Approach to Excellence and Trust*. Brussels, European Commission, 2020.
- Wigell, Mihael et al. (szerk.): *Geo-economics and Power Politics in the 21st Century*. London, Routledge, 2019.
- World Economic Forum AI Government Procurement Guidelines* (2019). Online: www.weforum.org/whitepapers/ai-government-procurement-guidelines.
- Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft* (2017). Online: www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.